UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,252	01/17/2001	James Russell Godwin	5577-220	8043

58505 7590 05/15/2006

STEVENS & SHOWALTER, L.L.P.
BOX IBM
7019 CORPORATE WAY
DAYTON, OH 45459-4238

EXAMINER	
PATEL, ASHOKKUMAR B	

ART UNIT	PAPER NUMBER
2154	

DATE MAILED: 05/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/764,252	GODWIN ET AL.	
	Examiner	Art Unit	
	Ashok B. Patel	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) *2,10-19,21,29-38,40 and 48-57* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9,20,22-28,39,41-47 and 58-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-63 are subject to examination. Claims 2, 10-19, 21, 29-38, 40 and 48-57 have been cancelled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 02/27/2006 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claims 1 and 58 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless-

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 3,4, 7, 20, 22, 23, 26, 39, 41, 42, 45, 58, 60, 61 and 63 are rejected under 35 U.S.C. 102(e) as being anticipated by Susai et al. (hereinafter Susai) (US 6, 411, 986 B1).

Referring to claim 1,

Susai teaches a method for providing secure communications over a network in a distributed workload environment (col. 3, line 62-67, "An interface unit can also be intelligent box sitting outside the server, in which case it can serve more than one server. The interface unit 202 can also be a load balancer, bandwidth manager, firewall, router, switch, computer system, or any other network device that is located between a client and server.") which are accessed through a distribution processor by a common network address (Fig. 2, element 202, col. 3, line 62-67, Fig. 7, col. 9, line 28-32, "According to this feature, interface unit 202 maintains connections with a plurality of servers, and routes client requests to these servers based on the path name specified in the client request."), the method comprising the steps of:

routing both inbound and outbound communications with target hosts which are associated with a secure network communication through the distribution processor (col. 9, line 48-58, "Interface unit 202 then translates the request and passes the translated request to the selected server, as shown in Step 708. This translation is described generally with respect to FIG. 4 above, and in detail below. The interface unit receives the response from the server, as shown in step 710. Interface unit 202 then translates the response and passes the translated response on to the client, as shown in step 712. As with step 708, the translation of step 712 is described in detail below.

Finally, interface unit 202 closes the connection with the client, as shown in step 714."); and

processing both inbound and outbound secure network communications at the distribution processor so as to provide network security processing of communications from the target host and network security processing of communications to the target host (col. 5, line 37-51, "Referring to FIG. 4, the network address of the packet is translated, as shown in step 402. In the case of an in-bound packet (that is, a packet received from a client), the source network address of the packet is changed to that of an output port of the interface unit, and the destination network address is changed to that of the intended server. In the case of an outbound packet (that is, one received from a server), the source network address is changed from that of the server to that of an output port of the interface unit, and the destination address is changed from that of the interface unit to that of the requesting client.").

receiving at the distribution processor, network communications directed to the common network address; (Fig. 7, col. 9, line 28-38, "According to this feature, interface unit 202 maintains connections with a plurality of servers, and routes client requests to these servers based on the path name specified in the client request. First, interface unit 202 opens connections with the servers, as shown in step 702. Next, in response to a client request, interface unit 202 opens a connection to the client and receives a request from the client to retrieve data using a path name, as shown in step 704.") and

distributing the received network communications to selected ones of the target hosts so as to distribute workload associated with the network communications (col. 9,

line 36-47, "Interface unit 202 selects the server hosting the content specified by the path name, as shown in step 706. In alternative embodiments, interface unit 202 consults other predefined policies to select the appropriate server, such as the load of the servers and the state of the servers. Interface unit 202 manages and maintains a database of servers and server farms that it tends. Among other things, information in this database includes currently active policies and rules that allow interface unit 202 to direct incoming packets to the correct server. Depending on network conditions and services desired, these policies and rules can change very quickly.")

Referring to claim 3,

Susai teaches a method according to Claim 2, further comprising the steps of: determining if the received network communications are secure network communications which are to be distributed to ones of the target hosts (col. 13, line 14-23, "Firewalls monitor packets and allow only the authorized packets to flow through. The present invention can be used to provide an additional feature within firewalls. Routers and switches also lie in the path of the network traffic. The industry trend is to integrate additional functionality (such as load balancing, bandwidth management and firewall functionality) within these devices. Hence, the present invention can easily be incorporated into a router.") wherein the step of processing both inbound and outbound secure network communications at the distribution processor comprises the step of processing the received network communications so as to provide generic communications to the ones of the plurality of target hosts if the received network communications are secure network communications which are distributed to ones of

the target hosts. (col. 3, line 64-67, "The interface unit 202 can also be a load balancer, bandwidth manager, firewall, router, switch, computer system, or any other network device that is located between a client and server.")

Referring to claim 4,

Susai teaches a method according to Claim 3, wherein the step of processing both inbound and outbound secure network communications further comprises the steps of: receiving at the distribution processor communications from the ones of the target hosts which are associated with secure network communications; and processing the received communications from the ones of the target hosts so as to provide network security for the communications from the ones of the target hosts.(col. 3, line 64-67, "The interface unit 202 can also be a load balancer, bandwidth manager, firewall, router, switch, computer system, or any other network device that is located between a client and server.", col. 13, line 14-23, "Firewalls monitor packets and allow only the authorized packets to flow through. The present invention can be used to provide an additional feature within firewalls. Routers and switches also lie in the path of the network traffic. The industry trend is to integrate additional functionality (such as load balancing, bandwidth management and firewall functionality) within these devices. Hence, the present invention can easily be incorporated into a router.", (col. 5, line 37-51, "Referring to FIG. 4, the network address of the packet is translated, as shown in step 402. In the case of an in-bound packet (that is, a packet received from a client), the source network address of the packet is changed to that of an output port of the interface unit, and the destination network address is changed to that of the intended

server. In the case of an outbound packet (that is, one received from a server), the source network address is changed from that of the server to that of an output port of the interface unit, and the destination address is changed from that of the interface unit to that of the requesting client."

Referring to claim 7,

Susai teaches a method according to Claim 4, wherein the communications received from the target hosts at the distribution processor and the generic communications to ones of the plurality of target hosts from the distribution processor are communicated over trusted communication links. (col. 3, line 64-67, "The interface unit 202 can also be a load balancer, bandwidth manager, firewall, router, switch, computer system, or any other network device that is located between a client and server.", col. 13, line 14-23, "Firewalls monitor packets and allow only the authorized packets to flow through. The present invention can be used to provide an additional feature within firewalls. Routers and switches also lie in the path of the network traffic. The industry trend is to integrate additional functionality (such as load balancing, bandwidth management and firewall functionality) within these devices. Hence, the present invention can easily be incorporated into a router.").

Referring to claim 20,

Claim 20 is a claim to a system that carries out the method of claim 1. Therefore, claim 20 is rejected for the reasons set forth for claim 1.

Referring to claim 22,

Claim 22 is a claim to a system that carries out the method of claim 3. Therefore, claim 22 is rejected for the reasons set forth for claim 3.

Referring to claim 23,

Claim 23 is a claim to a system that carries out the method of claim 4. Therefore, claim 23 is rejected for the reasons set forth for claim 4.

Referring to claim 26,

Claim 26 is a claim to a system that carries out the method of claim 7. Therefore, claim 26 is rejected for the reasons set forth for claim 7.

Referring to claim 39,

Claim 39 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 1. Therefore, claim 39 is rejected for the reasons set forth for claim 1.

Referring to claim 41,

Claim 41 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 3. Therefore, claim 41 is rejected for the reasons set forth for claim 3.

Referring to claim 42,

Claim 42 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 4. Therefore, claim 42 is rejected for the reasons set forth for claim 4.

Referring to claim 45,

Claim 45 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 7. Therefore, claim 45 is rejected for the reasons set forth for claim 7.

Referring to claim 58,

Susai teaches the method according to claim 1, wherein distributing the received network communications that directed to the common IP address among selected ones of the target hosts comprises:

Selecting among the target hosts for distribution of the network communications in response to a predefined selection pattern to distribute workload associated with the network communications among the target hosts.(col. 13, line 7-10, "Load Balancers which distribute client network connections between a set of servers in a server farm (local or geographically distributed). The invention can readily be combined with the load balancing function.", col. 9, line 38-47, "In alternative embodiments, interface unit 202 consults other predefined policies to select the appropriate server, such as the load of the servers and the state of the servers. Interface unit 202 manages and maintains a database of servers and server farms that it tends. Among other things, information in this database includes currently active policies and rules that allow interface unit 202 to direct incoming packets to the correct server. Depending on network conditions and services desired, these policies and rules can change very quickly."

Referring to claim 60,

Susai teaches the method according to claim 1, wherein distributing the received network communications that directed to the common network address among selected ones of the target hosts comprises:

Selecting among the target hosts for distribution of the network communications in response to a dynamic criteria that changes over a time to distribute workload associated with the network communications among the target hosts.(col. 13, line 7-10, "Load Balancers which distribute client network connections between a set of servers in a server farm (local or geographically distributed). The invention can readily be combined with the load balancing function.", col. 9, line 38-47, "In alternative embodiments, interface unit 202 consults other predefined policies to select the appropriate server, such as the load of the servers and the state of the servers. Interface unit 202 manages and maintains a database of servers and server farms that it tends. Among other things, information in this database includes currently active policies and rules that allow interface unit 202 to direct incoming packets to the correct server. Depending on network conditions and services desired, these policies and rules can change very quickly.")

Referring to claim 61,

Claim 61 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 58. Therefore, claim 61 is rejected for the reasons set forth for claim 58.

Referring to claim 63,

Claim 63 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 60. Therefore, claim 63 is rejected for the reasons set forth for claim 60.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5, 6, 8, 9, 24, 25, 27, 28, 43, 44, 46 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Susai et al. (hereinafter Susai) (US 6, 411, 986 B1) in view Basil et al. (hereinafter Basil) (US 6, 779, 051 B1)

Referring to claim 5,

Keeping in mind the teachings of Susai as stated above, Susai fails to teach a method according to Claim 4, wherein the communications received from the target hosts and the generic communications to ones of the plurality of target hosts are encapsulated in a generic routing format.

Basil teaches a method according to Claim 4, wherein the communications received from the target hosts and the generic communications to ones of the plurality of target hosts are encapsulated in a generic routing format. (Figs. 12A and 12B)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement the teachings of Basil into the

Interface/load balancer of Susai affording the GRE tunnel transmissions to the network endpoints such as Interface/load balancer of Susai.

It would have been obvious because Basil teaches not only GRE protocol at col. 1, line 8-26, "GRE is a protocol that enables the encapsulation of an arbitrary network layer protocol (the payload protocol) by another arbitrary network layer protocol (the delivery protocol). GRE tunnels are virtual tunnels that are created on an intermediary network and that are used to transmit GRE-encapsulated data packets from a first network to a second network. GRE tunnels are often used to create a virtual private network ("VPN") by connecting two remote local area networks ("LAN") via the Internet. At one end of a GRE tunnel, a router receives a payload packet from the first network, and encapsulates the payload packet so that it conforms to the delivery protocol of the intermediary network. The payload packet may be encapsulated in another packet or an Ethernet frame, for example. The encapsulated packet is transmitted through the intermediary network to the other end of the GRE tunnel. At that end, a router de-encapsulates the packet, and transmits the payload packet to the second network.", but also, depicts its implementations in Fig. 2, col. 3, line 21-40.

Referring to claim 6,

Keeping in mind the teachings of Susai, Susai fails to teach a method according to Claim 4, wherein the generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distribution processor and ones of the plurality of target hosts.

Basil teaches a method according to Claim 4, wherein the generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distribution processor and ones of the plurality of target hosts. (col. 5, line 10-19).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement the teachings of Basil into the Interface/load balancer of Susai affording the GRE tunnel transmissions to the network endpoints such as Interface/load balancer of Susai.

It would have been obvious because Basil teaches not only GRE protocol at col. 1, line 8-26, "GRE is a protocol that enables the encapsulation of an arbitrary network layer protocol (the payload protocol) by another arbitrary network layer protocol (the delivery protocol). GRE tunnels are virtual tunnels that are created on an intermediary network and that are used to transmit GRE-encapsulated data packets from a first network to a second network. GRE tunnels are often used to create a virtual private network ("VPN") by connecting two remote local area networks ("LAN") via the Internet. At one end of a GRE tunnel, a router receives a payload packet from the first network, and encapsulates the payload packet so that it conforms to the delivery protocol of the intermediary network. The payload packet may be encapsulated in another packet or an Ethernet frame, for example. The encapsulated packet is transmitted through the intermediary network to the other end of the GRE tunnel. At that end, a router de-

encapsulates the packet, and transmits the payload packet to the second network.", but also, depicts its implementations in Fig. 2, col. 3, line 21-40.

Referring to claims 8 and 9,

Keeping in mind the teachings of Susai as stated above, Susai fails to teach a method according to Claim 4, further comprising the step of establishing common IP filters for communications encapsulated in a generic routing format at the distribution processor and the plurality of target hosts, and a method according to Claim 8, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

Basil teaches a method according to Claim 4, further comprising the step of establishing common IP filters for communications encapsulated in a generic routing format at the distribution processor and the plurality of target hosts, and a method according to Claim 8, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format. (col. 5, line 31-34, Fig. 12A, element 160).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement the teachings of Basil into the Interface/load balancer of Susai affording the GRE tunnel transmissions to the network endpoints such as Interface/load balancer of Susai.

It would have been obvious because Basil teaches not only GRE protocol at col. 1, line 8-26, "GRE is a protocol that enables the encapsulation of an arbitrary network layer protocol (the payload protocol) by another arbitrary network layer protocol (the

delivery protocol). GRE tunnels are virtual tunnels that are created on an intermediary network and that are used to transmit GRE-encapsulated data packets from a first network to a second network. GRE tunnels are often used to create a virtual private network ("VPN") by connecting two remote local area networks ("LAN") via the Internet. At one end of a GRE tunnel, a router receives a payload packet from the first network, and encapsulates the payload packet so that it conforms to the delivery protocol of the intermediary network. The payload packet may be encapsulated in another packet or an Ethernet frame, for example. The encapsulated packet is transmitted through the intermediary network to the other end of the GRE tunnel. At that end, a router de-encapsulates the packet, and transmits the payload packet to the second network.", but also, depicts its implementations in Fig. 2, col. 3, line 21-40.

Referring to claim 24,

Claim 24 is a claim to a system that carries out the method of claim 5. Therefore, claim 24 is rejected for the reasons set forth for claim 5.

Referring to claim 25,

Claim 25 is a claim to a system that carries out the method of claim 6. Therefore, claim 25 is rejected for the reasons set forth for claim 6.

Referring to claims 27 and 28,

Claim 27 and 28 are claims to a system that carries out the method of claims 8 and 9. Therefore, claims 27 and 28 are rejected for the reasons set forth for claims 8 and 9.

Referring to claim 43,

Claim 43 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 5. Therefore, claim 43 is rejected for the reasons set forth for claim 5.

Referring to claim 44,

Claim 44 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 6. Therefore, claim 44 is rejected for the reasons set forth for claim 6.

Referring to claims 46 and 47,

Claims 46 and 47 are claims to computer readable medium having computer readable program code that carries out the method of claims 8 and 9. Therefore, claims 46 and 47 are rejected for the reasons set forth for claims 8 and 9.

8. Claims 59 and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Susai et al. (hereinafter Susai) (US 6, 411, 986 B1) in view Daoud et al. (hereinafter Daoud) (US 2002/0087694 A1)

Referring to claim 59,

Keeping in mind the teachings of Susai as stated above, Susai fails to teach the method of claim 58, wherein selecting among the target hosts for distribution of the network communications in response to a predefined selection pattern to distribute workload associated with the network communications among the target hosts comprises selecting among the target hosts associated with the common network address based on a round-robin pattern. (note: only the underlined limitations).

Daoud teaches these elements at page 2, para. [0024].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to implement the teachings of Daoud at the load balancer of Susai such that as Daoud put it, in para. [0024] FIG. 1 shows a load balancer 100 for routing a transaction 110 to a number of (i.e., one or more) servers 121, 122, 123 in a server pool 120. For purposes of illustration, Server A is unavailable as indicated by the "X" in FIG. 1. Using a simple "round-robin" approach, the load balancer" 100 receives a next transaction 110 and directs the transaction 110 to the next server in the server pool 120 (i.e., the last server to have received a transaction). For example, where the previous transaction is directed to server 123 (Server C), the next server is server 121 (Server A) even where the server 121 (Server A) is unavailable as shown in FIG. 1, and so forth."

Referring to claim 62,

Claim 62 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 59. Therefore, claim 62 is rejected for the reasons set forth for claim 59.

Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the

claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A. Follansbee can be reached on (571) 272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abp
***

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100